FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1514369-000

Total Deleted Page(s) = 15
Page 27 ~ Referral/Direct;
Page 28 ~ Referral/Direct;
Page 29 ~ Referral/Direct;
Page 30 ~ Referral/Direct;
Page 31 ~ Referral/Direct;
Page 32 ~ Referral/Direct;
Page 33 ~ Referral/Direct;
Page 34 ~ Referral/Direct;
Page 35 ~ Referral/Direct;
Page 36 ~ Referral/Direct;
Page 37 ~ Referral/Direct;
Page 40 ~ Duplicate;
Page 41 ~ Duplicate;
Page 46 ~ Duplicate;
Page 47 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

FD-224 (11-17-87)

BEHAVIORAL SCIENCE SERVICES ACCOMPLISHMENT REPORT

*To: MR. [redacted] *Date: 3/3/89 File#: QT 196B-1

☐ Foreign ☐ Domestic ☒ Bureau ☐ Other

*From: [redacted] Date of Activity: 3/2/89 Total Hours: 2

*Subject: [redacted]
AKA [redacted]
FRAUD BY WIRE;
OO: CHICAGO

Case Assigned To: [redacted] Unit Member (s): _____

* ☐ BSIRU ☐ BSISU ☒ BSCES ☐ POLICE FELLOWS

*Program: ☐ RESEARCH ☐ TRAINING ☐ VICAP ☒ PROFILE/CONSULTATION ☐ OTHER

* ☐ TELEPHONIC ☐ WRITTEN ☐ ON-SITE ☐ QUANTICO

Instruction Provided
- ☐ Field School
- ☐ Faculty Development
- ☐ Student Counselling
- ☐ Conference/Seminar
- ☐ Consultation
- ☐ New Agents
- ☐ National Academy
- ☐ DEA
- ☐ In-Service
- ☐ Preparation
- ☐ Role Playing
- ☐ Symposium
- ☐ Speaking Engagement
- ☐ Other _____
- ☐ Topic _____
- _____
- ☐ #Departments _____

Investigative
- ☒ Consultation
- ☐ Profile
- ☐ Personality Assessment
- ☐ Investigative Techniques
- ☐ Interview Strategy
- ☐ Trial Strategy
- ☐ Testimony
- ☐ Crime Analysis
- ☐ Equivocal Death
- ☐ #Victims ____
- ☐ #Subjects ____
- ☒ #Suspects 1

1 CONVICTION

VICAP
- ☐ Crime Analysis
- ☐ Consultation
- ☐ Linkage

Research
- ☐ Unpublished Paper/Handout/etc.
- ☐ Publication (Article/Book/etc.)
- ☐ Original Research/Academic Citation
- ☐ Interview
- ☐ Consultation

Administrative
- ☐ Meeting
- ☐ Media/Publicity
- ☐ Liaison
- ☐ Field Support
- ☐ Travel
- Time _____
- ☐ Consultation
- ☐ Psychological Service
- ☐ Organization Membership
- ☐ Awards/Honors/Letters
- ☐ Organizational Coop.
- ☐ Other _____

Computer Support
- ☐ Programming
- ☐ Data Analysis
- ☐ System Development
- ☐ Consultation
- ☐ Technical Assistance

Instruction Received
- ☐ In-Service
- ☐ Non-FBI

Other: _____

Project
- ☐ New
- ☐ Pending
- ☐ Closed

Class Description
#Of Students: ____ Student Type: _____ Instruction Hours: ____

196 B-1- 4

Distrib
1- Mr [redacted]
1- MR
✓ 1- QT 196B-1
1- QT 252C-C2187

Searched
Serialized
Indexed
Filed

FBI/DOJ

BEHAVIORAL SCIENCE SERVICES
NATIONAL CENTER FOR THE ANALYSIS OF VIOLENT CRIME
ACCOMPLISHMENT REPORT

*TO: MR. [redacted] *DATE: 10/5/87 FILE #: 196B-New

*☐ Foreign ☐ Domestic ☒ Bureau ☐ Other

*FROM: [redacted] *DATE OF ACTIVITY: _____ MANHOURS: 2

b6
b7C

*SUBJECT: [redacted]
aka [redacted]
FRAUD BY WIRE;
(OO: CHICAGO)

LOCATION: CHICAGO, ILL. CASE ASSIGNED TO: [redacted]

UNIT MEMBER(S): [redacted] ☐ BSIRU ☐ BSISU ☒ BSCES ☐ POLICE FELLOWS

PROGRAM: ☐ Research ☐ Training ☐ VICAP ☒ PROFILE/CONSULTATION ☐ OTHER

* ☒ TELEPHONIC ☐ WRITTEN ☐ ON-SITE ☐ QUANTICO

INSTRUCTION PROVIDED
- ☐ Field School
- ☐ Faculty Development
- ☐ Student Counselling
- ☐ Conference/Seminar
- ☐ Consultation
- ☐ New Agents
- ☐ National Academy
- ☐ DEA
- ☐ In-Service
- ☐ Preparation
- ☐ Role Playing
- ☐ Symposium
- ☐ Speaking Engagement
- ☐ Other_____

INVESTIGATIVE
- ☒ Consultation
- ☐ Profile
- ☐ Personality Assessment
- ☒ Investigative Techniques
- ☐ Interview Strategy
- ☒ Trial Strategy
- ☐ Testimony
- ☐ Crime Analysis
- ☐ Equivocal Death

VICAP
- ☐ Crime Analysis
- ☐ Linkage
- ☐ Consultation

RESEARCH
- ☐ Unpublished Paper/Handout/etc.
- ☐ Publication (Article/Book/etc.)
- ☐ Original Research/Academic Citation
- ☐ Interview
- ☐ Consultation

ADMINISTRATIVE
- ☐ Meeting
- ☐ Media/Publicity
- ☐ Liaison
- ☐ Field Support
- ☐ Travel Time_____
- ☐ Consultation
- ☐ Psychological Services
- ☐ Organization Membership
- ☐ Awards/Honors/Letters
- ☐ Organizational Cooperation

INSTRUCTION RECEIVED
- ☐ In-service
- ☐ Non-FBI

COMPUTER SUPPORT
- ☐ Programming
- ☐ Data Analysis
- ☐ System Development
- ☒ Consultation
- ☐ Technical Assistance

PROJECT
- ☐ New
- ☒ Pending
- ☐ Closed

#VICTIMS 1
#SUBJECTS 1
#SUSPECTS ___

OTHER: _____

(32)

OEA
196-New

196B-1-1

CLASS DESCRIPTION

Of Students: ___ Student Type: _____ Preparation Time: [redacted] Instruction Hours: [redacted]

b6
b7C

Distribution
- ☒ Program Manager
- ☒ Quantico Case File
- ☒ Employee Personnel Folder
- ☐ _____

Searched
Serialized
Indexed
Filed

*Mandatory Field

(DRAFT FORM)

SUMMARY: ON 10/2/87, SA [redacted] CHICAGO DIVISION, called b6 b7C
REFERENCE CAPTIONED CASE IN WHICH A 17 YEAR-OLD MALE WAS THE SUBJECT OF AN FBI/U.S. SECRET SERVICE INVESTIGATION. THE VIOLATIONS ARE BEING JOINTLY PURSUED BY FBI AND USSS, WHICH INCLUDE 18 USC SECTIONS 1030(a)(4); (a)(6) AND 641.

THE RESULTS OF A SEARCH OF THE SUBJECT'S HOME REVEALED COMPUTER EQUIPMENT AND STOLEN AT&T SOFTWARE, ESTIMATED TO BE WORTH $1 MILLION. THE SUBJECT ALLEGEDLY WAS TO HAVE OBTAINED ILLEGALLY THE AT&T SOFTWARE. THE INVESTIGATION ALSO PROBED THE POSSIBLE ATTEMPTS TO ACCESS U.S. GOVERNMENT COMPUTER SYSTEMS.

SA [redacted] CALLED THE NCAVC TO DETERMINE IF ANY b6 b7C PROFILES EXIST ON JUVENILE COMPUTER "HACKERS" AND IF ANY ADDITIONAL INFORMATION ON COMPUTER SECURITY EXISTED WHICH MAY PROVE USEFUL IN THIS INVESTIGATION. SA [redacted] WAS TOLD THAT SUCH A PROFILE DOES NOT EXIST AT THIS TIME.

SA [redacted] WAS SENT VIA BUMAIL THE FOLLOWING ITEMS: (1) AP WIRE SERVICE STORY ON CAPTIONED CASE; (2) A RECENT COPY OF 18 USC 1030; (3) ARTICLE FROM "COMPUTERWORLD 10/27/86; AND (4) A COMPUTERWORLD ARTICLE DATED 11/24/85 (ATTACHED)

THE SUBJECT IN THIS CASE HAS NOT BEEN ☐ See Attached CHARGED, PENDING CONSULTATION WITH LOCAL AUTHORITIES BY U.S. ATTORNEY.

COMMENTS/RECOMMENDATIONS:

OPEN AND ASSIGN THIS CASE TO [redacted] PENDING ANY b6 b7C FURTHER REQUESTS FOR ASSISTANCE.

FIELD OFFICE APPRAISAL:

*AUDIENCE:

*DEPARTMENTS:

ACTIVITY SPONSOR:

A* 18-Sep-87 11:31 [illegible]7 PM-ComputerBreak-In

KW: raid*

CHICAGO (AP) _ Investigators were led to a teen-age computer buff who tapped into NATO and Air Force base telephone networks after he sent messages using the code name "Shadow Hawk" that bragged of his actions.

In a Secret Service raid on the Chicago home of the 17-year-old hacker, agents confiscated his three computers and software stolen through AT&T company systems, said William J. Cook, an assistant U.S. attorney.

AT&T put the value of the software, some of which is not yet on the market, at more than $1 million.

Federal investigators now are analyzing piles of computer printouts to assess the damage before they decide whether to charge the youth.

There was no physical break-in, Cook said Thursday. The computer programs and other information were obtained by tapping into the systems by telephone, using another computer.

Shadow Hawk penetrated AT&T computers by disguising his own computer as a telephone company computer, then transferring company files into it, Cook explained.

Agents have been working full time since the Sept. 4 raid printing out "the enormous quantity of material stored in his computers," Cook said.

National security was not seriously jeopardized by the theft of material from an AT&T computer at NATO Maintenance and Supply Headquarters in Burlington, N.C., Cook said.

However, he declined to comment on the nature of information taken from an Air Force Base in Georgia.

The teen-ager also is suspected of revealing AT&T security devices over a computer network used as a kind of bulletin board for hackers.

The network, called "Phreak Class-2600," exists only "to educate computer enthusiasts ... to penetrate industrial and government sector computer systems," Cook said.

Authorities said they were led to the teen-ager partly through messages he left on the network bragging of having gained access to the AT&T computer files.

Kathryn Clark, a spokeswoman for AT&T, said the company's security systems were triggered by Shadow Hawk's break-ins.

An analysis of long-distance calls made from the youth's telephone indicates he also tried to enter computers at the accounts-payable department of the Washington Post and and other businesses, Cook said.

A 17-year-old is considered a juvenile, the prosecutor said, and if investigators believe charges are warranted, the Justice Department would be petitioned for permission or the case could be turned over to local officials for prosecution under state law.

Cook would not speculate on Shadow Hawk's motive, but he said some hackers, or computer buffs, like to see how far they can go with their machines.

S 1030. Fraud and related activity in connection with computers.

(a) Whoever--

(1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954, with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;

(2) intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

"(3) intentionally, without authorization to access any computer of a department or agency of the United Stated, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects the use of the Government's operation of such computer."

"(4) knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct futhers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer;

"(5) intentionally access a Federal interest computer without authorization, and by means of one or more instances of such conduct alters damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby-

"(A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; or

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; or

"(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if-

"(A) such trafficking affects interstate or foreign commerce: or

"(B) such computer is used by or for the Government of the United States;".

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is-

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(2)(A) a fine under this title or imprisonment for not more than one year, or both in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which does not occur after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment not more than ten years, or both, in the case of an offense under subsection (a) (2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under such subsection, or an attempt or commit an offense punishable under this subparagraph, and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which does not occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) or (a)(5) of this section which occurs after a conviction for another offense under such subsection, or an attempt to commit an offense punishable under this subparagraph;".

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the

United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section -

"(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

"(2) the term "Federal interest computer" means a computer-

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or

"(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;

"(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other possession or territory of the United States;

"(4) the term "financial institution" means-

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal home loan bank system and any home loan bank;

"(F) any institution of the Farm Credit System under the Farm Credit Act of 1971;

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934; and

"(H) the Securities Investor Protection Corporation;

"(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

"(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter; and

"(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5."

"(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States."

In Depth

New federal law bolsters computer security efforts

Computer crime laws deter unauthorized access • Should you report a computer crime? • Largest number of convictions — fraud by employees

By J. J. BUCK BLOOMBECKER

With the passage this month of a strengthened federal law, the Computer Fraud and Abuse Act of 1986 [CW Oct. 13] and new computer crime prohibitions in New York and Indiana, computer professionals can now use legal weapons against computer crime as never before. The federal government and most states now explicitly prohibit a range of computer crimes, which represents an unprecedented opportunity for the computer security professional to use the law as an adjunct of security policy.

So far, however, it seems that corporate and government victims of computer crime have shown little interest in going to court.

A computer crime census by the National Center for Computer Crime Data, a research institution in Los Angeles, was able to locate only 75 prosecutions pursuant to 38 states' computer crime laws. At a rate of fewer than two per state, the prosecution activity thus far is hardly frightening to a would-be embezzler. Though not as extreme as the Federal Bureau of Investigation's estimate that only one of 20,000 computer criminals goes to jail, the result of the census is nearly sufficient to encourage crimes. As long as criminals believe that the odds against punishment are great, their motivation will be accordingly great.

Using the criminal justice system to protect all of us is, to some extent, an obligation of citizenship as well as a time-tested social insurance strategy. Thus, one cannot discuss computer crime law without raising the major question every computer user must eventually face: Should we report a computer crime?

The importance of this question is underlined by the fact that short-term, narrow self-interest may well dictate a strategy opposite to that of long-term social responsibility. A number of victims of computer crime have confided, for example, that they did not report and prosecute computer crime cases because of embarrassment.

Another explanation is that it seldom seems cost-effective to be involved in a computer crime prosecution. The time involved in assisting prosecutors and investigators, the amount of unfavorable publicity a trial may involve and the relatively low probability that the defendant will make full restitution — all of these factors make it easy for a computer crime victim to conclude that the costs of prosecution outweigh the benefits.

But from another perspective, there must be a investment of faith in the criminal justice system as a preventer and detector of computer crime, or else the system will have no deterrent effect at all.

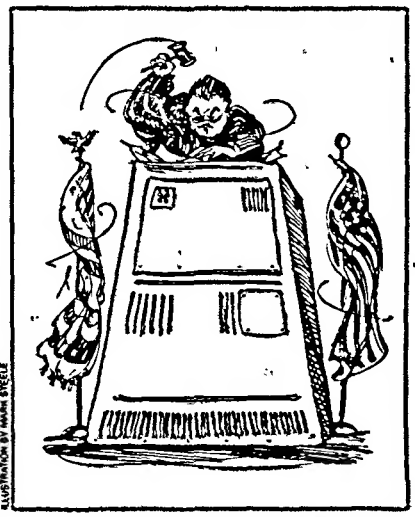


ILLUSTRATION BY HANK STEELE

Knowing exactly what the law prohibits should facilitate more informed — and ideally more responsible — reactions in the increasingly likely event that your computer system becomes the scene of a computer crime. What follows is a summary of the provisions of the federal and state computer crime laws, based on the ongoing research of the National Center for Computer Crime Data.

'Democratization' defined

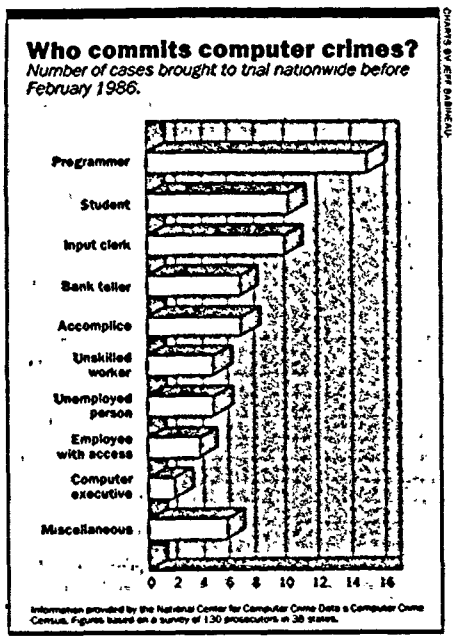
Computer crime is becoming increasingly likely because computer technology is becoming more accessible. It is, unfortunately, becoming "abuser friendly." We call this trend the democratization of computer crime.

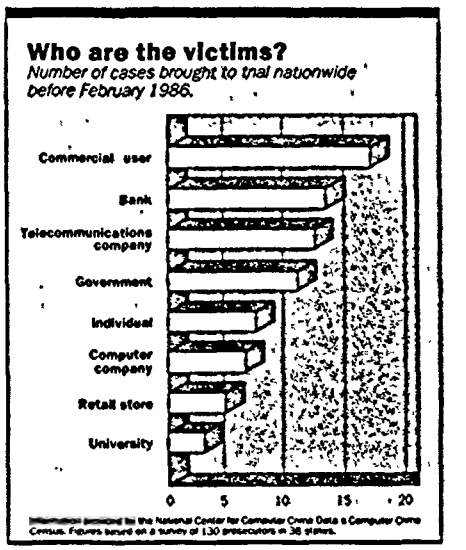
Democratization is the spread of computing to a far larger segment of the population in the last several years. With it has come a consequent increase in opportunities for anyone who wants to become some sort of computer criminal. Further — and unfortunately without any element of choice — virtually anyone can now become a computer crime victim.

The technology of computer crime has been democratized to the point where a modem, the most commonly used tool for hacking, can easily be bought for less than $500. And many computer criminals have received on-the-job training. Employees represent a far more significant computer crime threat than do juveniles or traditional criminals. The number of potential employee criminals grows as more jobs

About the author

BloomBecker is director of the National Center for Computer Crime Data, a nonprofit research institute in Los Angeles. An extended version of this article will appear in the November supplement to Datapro Reports on Information Security.





involve computer use.

The largest category of defendants in the National Center for Computer Crime Data survey was employees. Included here are programmers, bank tellers, input clerks and other employees with access to their companies' systems.

Employees represent a continual threat, since they have far greater ability to do damage and far more system-specific information to base their efforts upon.

In addition, they often have more of a financial motive to commit a crime and often more psychological motivation to hurt the chosen victim.

Cases of malicious damage to computer systems are primarily cases involving employees or former employees.

Within the general category of employees, consultants as a group also stand out as particularly noticeable in the computer crime cases the National Center for Computer Crime Data has studied.

The computer crime census did not break out information on consultants, so no exact figures are available. However, the raw data suggests that a number of the programmers counted were actually consultants or temporary employees hired to do a specific job.

In many cases these work relationships were poorly defined in the employment contract, or there was no written contract at all.

Without in any way implying that all consultants are to be feared — no more than it is implied that all employees or all youths are to be feared — it is important to note that in a number of cases, individuals from outside a company gained information in the course of consulting work and then used the information against the company through a computer crime.

One such case was the case of Stanley Mark Rifkin, who stole $10.2 million from the Security Pacific National Bank using his knowledge of its wire transfer system, which he gained while he was working for the bank.

In another case, a consultant who was hired to assist a company in gaining the necessary environmental and zoning permits to begin manufacturing computer disks threatened to sell the formula for the production of disks to a competitor unless his employer paid him a ransom. He was easily convicted when he made his offer to an FBI agent posing as an agent of his company.

Computer crime laws are our nation's reaction to the types of computer crimes that have been reported and that it is feared will occur in the

> ***The goal of these laws is to define those acts that will be punished in hope that the threat of punishment will deter some individuals from committing the acts.***

future. The goal of these laws, I believe, is to define those acts that will be punished in hope that the threat of punishment will deter some individuals from committing the acts. The purpose of this section is to summarize the types of acts that the computer crime laws attempt to combat.

Money theft. Many computer crimes involve theft of money. These range from complex bank frauds like the Wells Fargo theft to simple, even trivial falsifications of records that allow money to be misappropriated. It is the "big-killing" case that legislative testimony focuses on primarily, since few manual system crimes involve sums as large as those in the Equity Funding case, in *U.S.* v. *Riffkin* or in *U.S.* v. *Smith, Lewis and Marshall.*

Service theft. Use of computer services for one's own benefit may be for commercial or noncommercial purposes. An example of the latter is the case of a programmer who kept private files on the New York City Board of Education computer. He was found not guilty because the state theft of services law was held not to apply to his actions.

In contrast, in Indiana, a county employee was convicted of theft under the state's new criminal code for using less than 10 dollars' worth of the memory of a county computer system.

A case involving a Long Island, N.Y., university computer system demonstrates the commercial use of computer services. In this case, the manager of the computer center and his assistant used the school's computer to service commercial accounts for their own enrichment. They received at least $53,000 in revenue from one of their clients.

Program and data theft. Data and programs are themselves valuable property and thus are the subject of theft from computer systems. Employees have been charged with computer crime or trade secret theft on several occasions involving disputes between employee and employer as to what the employee is entitled to take upon leaving the company. In a number of these cases, the ex-employee is now employed in, or the owner of, a competing business.

Data alteration. Some changes in data allow criminals to derive significant gains, tangible or intangible. A recent prosecution in Los Angeles resulted in a guilty plea by an employee of the University of Southern California who had been taking payments from students and changing their grades in return.

Other reported schemes involved changes in credit information and changes in department of motor vehicles records that facilitated the theft of the cars to which the records referred.

Program damage. Programmers familiar with a system can do considerable harm by erasing or replacing parts of major programs.

A recent case involved a plan to erase the operating systems of two computers maintained by a Los Angeles corporation that operated several restaurants and fast-food outlets.

In another case, a "logic bomb" was used to interfere with operations at the Department of Water and Power in Los Angeles. A logic bomb is a program that causes a computer system not to operate as it should.

Data destruction. Mostly as acts of mischief, contents of files have been destroyed. In San Francisco, United States Leasing International, Inc. found that several people replaced words in their files with curse words, friends' names and similar material.

Malicious access. One of the leading issues in reaction to hacking is the problem of what to do when a hacker gets access to a computer system, reads some files but neither steals nor damages anything. This situation is becoming increasingly common in the computer crime cases that are prosecuted.

In California, a court found that the typical computer crime statute language prohibiting "malicious" access to a computer system did apply to users gaining access to others' computer systems. In some of the charges against the defendant in this case, there was evidence of not just access but also of damage to the computer system.

Violation of privacy. A consistent fear relating to computers is that the computer will facilitate invasions of privacy. Some jurisdictions — particularly in Europe, where privacy protection is more advanced — use administrative law to protect privacy more frequently than they use criminal law.

With the growing awareness of the dangers that computer crime poses to average citizens, it can be anticipated that invasions of privacy will increasingly be punished through the use of computer crime law. Several examples of this sort of prosecution already exist.

What assets do the laws protect?

Criminal law can be seen as the way in which society defines which assets it will protect. Thus the definitions contained in the computer crime laws are important because they make clear the extent to which computer crime law will protect the items with which a data processing professional comes in contact.

The common law frequently limits the definition of property to tangible items. Where computers are involved, this limitation is significant. Much of the value in a computer system consists of intangibles — especially data and programs.

Some of the most difficult issues in computer crime litigation involve the fact that much of the computer's operation consists of changes in electrical charge on various media or reproduction of those charges.

These electrical charges are not traditionally considered tangible, and there is considerable question as

A summary of the 47 state computer crime laws

	Class of crime*	Generally	To obtain property	Hardware	Software	To obtain property	Computer items	Data	Access codes	Services	Services	Critical services	Other
			Access or use			Alter, damage or destroy			Alter, take or disclose			Disrupt or deny	
Ala.	M,F	▪	▪	▪	▪	▪		▪			▪		
Alaska	M,F	▪						▪[2]		▪	▪		Deceive a machine
Ariz.	F	▪	▪	▪	▪	▪							
Calif.	M,F	▪	▪	▪	▪								
Colo.	M,F	▪	▪	▪	▪								
Conn.	M,F	▪		▪				▪[2]		▪	▪		
Del.	M,F	▪		▪				▪[2]		▪	▪		
Fla.	M,F			▪	▪	▪					▪	▪	
Ga.	F	▪	▪	▪	▪			▪[2]					
Hawaii	M,F	▪	▪	▪	▪			▪[2]					
Idaho	M,F	▪	▪	▪	▪								
Ill.	M,F	▪	▪		▪								
Ind.	M,F	▪			▪								
Iowa	M,F	▪	▪	▪	▪								
Kan.	M,F	▪	▪	▪	▪								
Ky.	M,F	▪	▪										Conceal computer information
La.	M,F		▪	▪	▪			▪					
Maine	▪									▪			
Mass.	▪							▪[2]			▪		
Md.	M	▪						▪[2]					
Mich.	M,F		▪	▪	▪								Use to commit other crimes
Minn.	M,F		▪	▪	▪								
Miss.	M,F		▪	▪	▪				▪				
Mo.	M,F	▪	▪	▪	▪	▪		▪[2]				▪	
Mont.	M,F	▪	▪		▪								
N.C.	M,F		▪					▪					Extortion
N.D.	F	▪	▪	▪	▪	▪							
Neb.	M,F	▪	▪	▪	▪			▪[2]			▪		
Nev.	M,F		▪	▪	▪							▪	
N.H.	M,F	▪		▪				▪		▪	▪		
N.J.	M,F		▪	▪	▪			▪					
N.M.	M,F		▪	▪	▪								
N.Y.	M,F	▪	▪[3]		▪	▪[3]	▪[3]						Receiving copies of material
Ohio	F	▪	▪					▪			▪		
Okla.	M,F	▪	▪										
Ore.	M,F		▪	▪	▪					▪			
Pa.	M,F	▪	▪									▪	
R.I.	F		▪	▪	▪		▪						
S.C.	F		▪	▪	▪		▪				▪		
S.D.	M,F	▪	▪		▪				▪				
Tenn.	F		▪	▪	▪								Conceal computer information
Texas	M,F	▪		▪	▪				▪				
Utah	M,F		▪	▪	▪	▪	▪	▪			▪		
Va.	M,F				▪		▪	▪[2]		▪	▪		Forgery
Wash.	M,F	▪			▪								
Wis.	M,F	▪		▪	▪		▪		▪				
Wyo.	M,F			▪	▪	▪		▪[2]				▪	

* Misdemeanor (M) or felony (F)
[1] Private data
[2] Trade secret
[3] Credit data
[4] Public records
[5] Computer material
[6] Copying computer material
[7] Financial data

Information provided by the National Center for Computer Crime Data. 'Computer Crime Law Reporter'

Every state except Arkansas, Vermont and West Virginia has enacted computer crime laws. Though they unanimously classify violations as criminal, the different state laws vary widely in the acts they forbid and the penalties they mete out.

to whether computerized data falls within the traditional legal concepts of property.

Thus, if one could steal information without taking anything physical, it could be (and in some courts has been) deemed that there has been no "taking" that is sufficient to constitute theft. The definitions used in the computer crime laws appear to aim at reducing this problem.

For example, a group of private insurance investigators took doctors' files without authorization, copied the contents of the files and then returned them. The investigators were prosecuted for theft, and their case was dismissed.

The Colorado Supreme Court ruled that since the investigators had no intent to permanently deprive the owners of the files of anything and sought only the intangible information the files contained, the Colorado theft law did not authorize prosecution for theft. Analogously, many malicious mischief statutes prohibit only damage to "real or personal property."

It is not at all clear that electrical impulses on a computer medium are real or personal property or that a change in the impulse is damage to the medium itself.

For reasons such as this, there are provisions in virtually all computer crime laws that define property much more broadly, including intangible data, software as well as information.

What acts are prohibited?

The 47 state computer crime laws and the two federal computer crime laws that have been passed in the last decade are reactions to a number of perceived and actual difficulties in applying common law criminal prohibitions to the types of interferences with computer systems that have been discussed above.

The fears motivating the institution of these laws revolved around the possibility of criminal behavior involving the computer either as the target of a crime or as the vehicle through which a crime might be committed.

Most state laws, and the federal laws discussed below, can be divided into four categories: definitions of computer assets, definitions and prescriptions of criminal behavior, punishment provisions and ancillary provisions.

The following summary attempts to describe the behavior forbidden by the various laws (see chart p. 52), the types of computer assets that are protected by the laws and a number of the details that determine the application of these laws to specific fact situations.

Federal computer crime law

At the end of 1984, the first federal computer crime law was passed. This bill was a compromise version of H.R. 5616, criminalizing unauthorized access to classified national security information or information in certain financial records.

Additionally, certain unauthorized access to computers operated on behalf of the government was criminalized.

This month, the second federal computer crime law was passed. This bill, called the Computer Fraud and Abuse Act of 1986, or H.R. 4718 in its House version, is the result of further hearings into the problem of computer crime by the House Committee on the Judiciary and the Senate Judiciary Committee.

> ***The definitions contained in the computer crime laws are important because they make clear the extent to which computer crime law will protect the items with which a data processing professional comes in contact.***

Mindful of questions of separation of power, the first federal computer crime bill did not extend its coverage to computers operating in interstate commerce.

The 1986 bill protects these computers against access with intent to defraud, access resulting in more than $1,000 loss and access to certain medical computer systems. It also prohibits trafficking in computer access passwords, which affects interstate commerce.

The more extended coverage was originally dropped in order to reach a compromise with legislators who hesitated to expand federal jurisdiction before further study demonstrated the need for it.

But after the 1986 hearings, Congress apparently felt that this expansion of jurisdiction was appropriate. The current computer crime law defines action as criminal if an individual does the following:

- "Knowingly . . . obtains information that has been determined by the U.S. Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . or any restricted data."
- "Intentionally . . . obtains information contained in a financial record of a financial institution . . . or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act."
- "Intentionally accesses a computer without authorization if such computer is exclusively for the use of the Government of the United

States or, in the case of a computer not exclusively for such use, if such computer is used by or for the Government of the United States and such conduct affects such use."

• "Knowingly and with intent to defraud, accesses a Federal interest computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer."

• "Intentionally accesses a federal interest computer without authorization, and by means of one or more instances of such conduct alters information in that computer, or prevents authorized use of that computer, and thereby causes loss to one or more others of a value aggregating $1,000 or more during any one-year period, or modifies or impairs . . . the medical examination . . . diagnosis . . . treatment . . . or care of one or more individuals."

• "Knowingly and with intent to defraud trafficks . . . in any password or similar information through which a computer may be accessed without authorization if (a) such trafficking affects interstate or foreign commerce; or (b) such computer is used by or for the Government of the United States."

The 1986 computer crime law has eliminated an inconsistency between most state laws and the 1984 federal law. Like the state laws, the 1986 law explicitly criminalizes attempts and conspiracies to commit the crimes defined in the federal law.

Defining terms

Unlike the state laws based on either the Florida model or the Federal Computer Systems Protection Act (S. 1766), the new Section 1030 of Title 18 U. S. Code defines only six terms, three of them in ways relevant only to federal law.

It defines "computer" in a very extensive manner, including "electronic, magnetic, optical, electrochemical or other high-speed data processing device(s)." The definition of computer includes data storage or communications facilities directly related to, or acting in conjunction with, a computer.

A "federal interest computer," which is protected in Sections 4 and 5 of the bill, is defined as "one of two or more computers used in committing the offense, not all of which are located in the same state." In addition, Section 6 contains an even broader jurisdictional standard, where the criminal offense "affects interstate or foreign commerce."

Federal law defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter

> ***Mindful of questions of separation of power, the first federal computer crime bill did not extend its coverage to computers operating in interstate commerce.***

> ***The widespread use of computers, especially by employees, has been responsible for a number of provisions that indicate that any authorized use of a computer cannot give rise to liability.***

information in the computer that the accessor is not entitled so to obtain or alter." The other terms defined are "state," "financial institution" and "financial record."

The federal law currently prohibits access to computer systems that is "knowing" (in paragraph 1), "intentional" (in paragraphs 2, 3 and 5) or "knowing and with intent to defraud" (in paragraphs 4 and 6) and without authorization or beyond authorization.

The House Judiciary Committee report on the 1986 Computer Fraud and Abuse Act explains that the shift from "knowing" to "intentional" access was designed to add "a slightly higher state-of-mind standard" to the law.

State laws

In interpreting the variety of state computer crime laws on the books, "intent" is often a key. The four important issues that concern the intent with which a computer crime is alleged to have been committed are knowledge, purpose, malice and authorization. As in most of the criminal law, computer crime law requires at the very least an awareness of what the person committing the crime is doing.

This knowledge is expressed by different words in different statutes. Included are the terms "knowing," "willful" and "intentional."

In the absence of judicial interpretations to the contrary, it appears appropriate to interpret all of these words to mean that the actor knows what he or she is doing.

Legally, this knowledge need not necessarily extend to the actual consequences of one's actions, as long as those consequences are reasonably foreseeable from the actions that were known.

For instance, members of the "414 gang" testified that they would try to get access to computer systems when they did not know the identity of the owners of those systems. Thus, they could argue that unless a certain computer system contained an introductory message alerting them that the system prohibited unauthorized access, they would have no way of knowing that such was the case.

In contrast to the former terms, the use of the word "purpose" in many computer crime laws would appear to require proof that someone charged under those laws had a specific intent to commit a certain type of crime.

Consider the language that says "Any person who ... accesses ... a computer ... for the purpose of devising any scheme or artifice to defraud ... is guilty of a computer crime." Knowingly getting access into a computer system without the intent to devise a scheme to defraud would not be a crime under this language.

If, for example, a hacker only wants to look around, not to change data, steal anything or otherwise disrupt the system, he or she would not be liable under such a provision.

Malice

Malice is generally interpreted as meaning a specific intent to do harm. Using the hacker example again, it would appear to be a defense to a statute forbidding "malicious" access to a computer system to prove that the accused did not intend to do harm.

For example, the defendant in *Hoppe v. Austin* contested this issue in a case recently concluded in Los Angeles. In response to the charge that he had maliciously accessed a number of computer systems, Austin argued that his accesses were not meant to harm any of the

Invisible safecrackers: Today's thieves work through wires

Electronic banking spawns highly lucrative crime wave

By AUGUST BEQUAI

One weekend in 1965, a gang of safecrackers used a 70-mm. antitank gun to blast their way into a Brink's vault in Syracuse, N.Y. They made away with about $300,000.

Today's successful safecracker has gone electronic. As vaults give way to electronic funds transfer (EFT) systems, security experts are concerned that EFT thefts could run into the trillions of dollars. A bank security officer once remarked, "It's something that really scares us. It's frightening."

EFT makes police and banking officials nervous and with reason. More than $2 trillion moves daily through global EFT networks. Automated teller machines (ATM) alone handle more than three billion transactions involving $250 billion annually. But the Interbank Card Association, which represents the Mastercard system and other banking groups, fears that ATMs are vulnerable to theft.

The U.S. Department of Justice has already identified four areas in which EFT systems are vulnerable: unauthorized use of access devices, frauds by authorized users, internal manipulations by dishonest employees and sabotage. The federal government, the biggest user of EFT systems, is particularly concerned with the manipulation of these systems by dishonest insiders. As illustrated by the following examples, others share this concern:

- In Switzerland, a gang of electronic thieves intercepted an EFT transmission and diverted the funds to their own accounts.
- In Japan, a communications engineer with the Nippon Telephone & Telegraph Co. tapped a bank's EFT lines and gained access to the account numbers of its cash-card customers. Armed with these and counterfeit cards, he took the bank for more than 170 million yen before being discovered.
- In the U.S., a bank data entry clerk stole more than $25,000 in a two-month period simply by manipulating the automated central information files. This enabled him to access customer accounts through the bank's ATMs.

According to the American Bankers Association, more than 60% of the 225 banks that it surveyed had been the victim, at least once, of an EFT fraud. Many of the offenses had been committed by dishonest insiders.

A series of hearings on EFT systems by the U.S. House Banking Committee came up with a number of findings. First, "remote muggings" involving ATMs were becoming a problem. Thieves were finding it lucrative to rob people who had just withdrawn money from ATMs. Also, the theft of ATM cards and codes had become commonplace. Next, impersonating bank officials, thieves were telephoning banks and their customers to obtain secret codes. Lastly, dishonest customers were making withdrawals while claiming they had lost their ATM cards.

Although there is mounting evidence that EFT crimes are increasing, a consensus has not yet been reached on what exactly constitutes an EFT crime or on the scope of the problem. Suffice it to say that these crimes are unlawful acts directed at — or making use of — one or more EFT systems. Annual losses attributed to EFT crimes are said to range anywhere from 100 million to several billion dollars, depending on the source.

Computer crime has been in the limelight of criminology in recent years, and EFT thefts and frauds, one of its offshoots, has recently been scrutinized by such groups as the American Bankers Association and various law enforcement and congressional commitees. From these sources and from the crimes that have surfaced, we find that EFT offenses can take the following forms:

- Physical attacks directed at EFT systems or any of their components.
- Robberies, thefts and other attacks that are directed at users of these systems.
- Unauthorized use of access devices such as cards, plates, codes, account numbers, passwords or any other device used to gain access to an account.
- Fraud and thefts by authorized users in which, for example, the user falsely claims that a third party used his access device to make withdrawals from his account.
- Frauds and thefts by dishonest insiders: Armed with a customer's card and personal identification number, these thieves carry out unauthorized withdrawals and transfers.
- Thefts based on error — that is, situations in which a dishonest customer steals funds erroneously deposited in his account.
- Unauthorized transactions by outsiders, often carried out with the help of dishonest employees.
- Blackmail, especially in cases in which the account holder occupies a sensitive political position.
- Manipulation of data, often involving the internal manipulation of the system's software or hardware.
- Extortion, especially when terrorists and other political extremists are involved.
- Electronic interceptions, often directed at a system's communications lines.
- Counterfeiting of access devices, a carryover from the credit card industry.

> *One selling pitch of the cashless society is that it will serve to curtail crime. However, it has spawned new, more costly crimes.*

In part, the lack of valid data in the area of EFT crime must be attributed to the financial industry. Fearful that it might scare away existing or potential EFT customers, the industry has often swept the problem under the rug. The financial community does, however, recognize the threat of EFT crime. Efforts are underway to educate EFT users on the need for security and to enact state laws that would facilitate the prosecution of EFT criminals. The U.S. Congress just passed a law making it a federal crime to misuse access devices.

New security devices are also hitting the market. For example, plans are afoot to improve access security through the use of fingerprint scanners. A scanner would compare the user's fingerprints with those stored in digital form in the bank's computer. Depending on whether the prints matched, it would either permit or deny access to the system. Chemical Bank, First Interstate and Wells Fargo Bank, N.A. are exploring their possible use.

There are also plans to replace present EFT cards with smart cards — "plastic money that talks." First test-marketed in Europe, the card contains a tiny memory and a microcomputer in a silicon chip that is the size of a small coin. The microchip contains both the customer's account number and credit limit; data can be encoded on it for up to 180 separate accounts.

The smart card is not without its drawbacks. It is costly to produce — more than $15, as compared with 65 cents for the type of cards currently used.

Also under consideration are such safeguards as voice identification, hand pattern identification and signature identification. All of these are costly and safeguard only entry into the system, not the total system. They must be viewed as merely the beginning in a long and drawn-out process to make EFT systems secure.

One of the selling pitches of the cashless society has been that it will serve to curtail crime. By that, its proponents must obviously mean traditional crime, since the cashless society has already spawned new and more costly crimes. Difficult to detect and guard against, these crimes pose a challenge to the viability of the financial sector — one that we have yet to address.

As is the case with computer crime, a lack of confidence in the ability of our criminal justice system to address these offenses only serves to reinforce the financial industry's reluctance to come forth and assist in identifying these offenses. Often when frauds surface, a financial institution's practice is to refer them to its in-house security staff for disposition. The wide variety of definitions and procedures used by banks to record these frauds makes it easy to mask the crimes.

We need to determine both the prevalence and characteristics of these crimes if we are to address the problem. Without these, the task of developing safeguards and laws to tackle the problem could prove difficult, if not futile.

Security is an important first step in securing EFT systems. But of even greater importance is the need to carefully scrutinize the cashless revolution. Its impact and implications for our society are too great to be left solely in the hands of the financial community. ■

computer systems and thus were not malicious.

His argument, however, was unsuccessful, and after a court trial, he was incarcerated for a presentence probation examination and then placed on felony probation.

Nonmalicious access

In order to eliminate the requirement of malice, some statutes have been drafted explicitly to punish nonmalicious access. Subsequent to the filing of the Austin case, for example, California added a computer trespass section to its computer crime law. It prohibits entry into a computer system that is knowing and without authorization, but not malicious.

In another example, New Jersey law includes a provision defining as a "disorderly person" one who "purposely and without authorization accesses a computer, ... and this action does not result in altering, damage or destruction of any property or services."

A number of statutes indicate that only "unauthorized access" to computer systems can be punished. Some statutes explicitly define authorization. Colorado, for example, defines authorization as "the express consent of a person which may include an employee's job description to use said person's computer, computer network, computer program, computer software, computer system, property or services."

Defenses

A number of the computer crime laws include provisions that can be used as defenses by those accused of computer crime. The widespread use of computers, especially by employees, has been responsible for a number of provisions that indicate that any authorized use of a computer cannot give rise to liability. As shown above, many of the statutes do this directly in their definition of computer crime by prohibiting only unauthorized acts.

Connecticut law explicitly creates "authorization" as an affirmative defense, providing that: "It shall be an affirmative defense to a prosecution for unauthorized access to a

> *The determination of the punishment in a specific case will depend on the type of crime, type of harm, existence of enhancement provisions, existence of multiplier provisions and civil remedies.*

computer system that a person reasonably believed that the owner of the computer system, or a person empowered to license access thereto, would have authorized him to access without payment of any consideration, or that person reasonably could not have known that his access was unauthorized."

Analogously, though not quite so clearly, California appears to create a defense for computer access done in the course of one's employment.

It provides that "any person who intentionally and without authorization accesses any computer system . . ., with knowledge that the access was not authorized shall be guilty of a public offense. This subdivision shall not apply to any person who accesses his or her employer's computer system, computer network, computer program or data when acting within the scope of his or her employment."

The New York law allows as a defense the argument that the defendant had reasonable grounds to believe he or she was authorized to use a computer, to alter its data or to copy data or programs.

Texas law exempts employees of communications common carriers as well as electric utilities from liability, so long as their actions were in the course of employment and necessary to protect the property of their employer.

Kansas law makes it a defense if "the property or services were appropriated openly and avowedly under a claim of title made in good faith."

Punishment

The range of punishment for computer crime is immense. It ranges from infraction treatment in California requiring the payment of a small fine to prison sentences as long as 10 years and fines that can be as much as $100,000 in Oklahoma.

The determination of the punishment in a specific case will depend on the type of crime, type of harm, existence of enhancement provisions, existence of multiplier provisions and civil remedies.

The provisions of the 1986 law make significant changes in the structure of punishments for federal computer crimes.

Crimes involving access to classified information can be punished by a fine and/or 10 years' imprisonment.

The earlier bill's provision that the fine could be up to twice the value obtained by the offense has been dropped, and now the general provisions of the Criminal Fine Enforcement Act of 1984 govern the allowable fine.

Further, second offenses can be punished with 20 years of imprisonment and/or a fine.

Violations of Section 3 of the 1986 law dealing with unauthorized access or Section 6, dealing with trafficking in passwords, can be punished with imprisonment for one year or less and/or a fine.

The same offenses or violations of Section 2, dealing with financial records, can be punished with imprisonment for not more than 10 years if there has been a prior conviction for the same crime.

Violations of Section 4, dealing with computer access with intent to commit fraud, or Section 5, dealing with alteration of computer information or interference with computer use, can be punished with up to five years imprisonment and/or a fine.

A prior conviction under

Sections 4 or 5 can increase the imprisonment to a term of 10 years.

Attempts are treated the same as completed crimes for purposes of punishment.

Valuation

One of the difficult issues in computer crimes is valuation. If the asset that has been damaged or taken can be freely traded — like a personal computer or even a custom-made computer program — then calculating the market value of the lost or damaged asset is usually adequate. Other cases are not so easily measured.

A variety of measures of value are found in the computer crime laws:

- Connecticut sets value at the market value or replacement cost at the time of violation.
- Iowa calls the value of property taken or destroyed "loss" and defines it as the retail value or replacement or repair cost, whichever is less.
- Montana has a definition similar to Connecticut's. It includes the following: "The value of electronic impulses, electronically produced data or information . . . or any other tangible or intangible item relating to a computer . . . shall be considered to be the amount of economic loss that the owner of the item might reasonably suffer by virtue of the loss of the item. The determination of the amount of such economic loss includes but is not limited to consideration of the value of the owner's right to exclusive use or disposition of the item."

Unresolved Issues

As indicated above, democratization has been the biggest change in the computer crime landscape in the last few years. The most significant consequence is the fact that hacking remains more of a problem than ever before.

The primary problem is the relative youth of the participants and the seriousness of the potential damage they can do.

Federal law is virtually useless where juveniles are concerned. Before a juvenile is tried in a U.S. federal court, the attorney general of the U.S., after investigation, must file a certificate asserting that the juvenile court or other appropriate state court does not have jurisdiction in the case or that it refuses to assume jurisdiction — or that the state juvenile system does not have available programs and services that are considered adequate for the needs of the juvenile.

As a practical matter, this has meant that virtually all juveniles who are arrested by the FBI have been released or have been referred to the local police for prosecution.

Few federal cases have been brought against these juveniles.

A related question is one of forming an appropriate corporate policy to deal with minors. There are significant differences of opinion about the ideal degree of freedom that young computer enthusiasts should be allowed in their interaction with mainframes.

A policy for minors

While all responsible commentators agree that doing serious damage by changing data or programs is wrong, other questions are more difficult:

- Should hackers be hired to investigate computer crime?
- Will better security simply lead to more efforts by hackers to break a computer system's security?
- What is the appropriate punishment for someone who is convicted of hacking?

The company contemplating taking action against a young computer user also will want to avoid the appearance of overreaction that seemed to accompany the raids by the FBI in August 1983, when its agents seized the computers of 15 teenagers.

Another case represents the need for careful attention to the impressions that may result from poorly considered prosecution decisions, for example, the Tcimpidis case that was prosecuted in Los Angeles in 1984 and 1985.

In this case, a systems

CORRECTION

The correct name of the systems integrator mentioned in the story on the American Association of Retired Persons [In Depth, Oct. 6] is American Management Systems, Inc.

operator was charged with a crime for "publishing" a telephone company credit card number.

There was no allegation that he had posted the number on the bulletin board system that he ran, but only that the act of operating his system made him a publisher of all the information contained on it.

The case drew considerable attention, since it suggested a broad range of criminal liabilities for operators of bulletin boards.

The comment of the telephone company representative — that next time he would pick someone who was really guilty — did little to reassure those in the public who considered the case as an attempt by the phone company to reduce the spread of bulletin boards.

> *"In the future, computer professionals can expect to be increasingly challenged to define their responsibility for the security of computer systems."*

In the future, computer professionals can expect to be increasingly challenged to define their responsibility for the security of computer systems.

Otherwise, they will find others defining the responsibility for them.

Take the initiative

A California case alleged that TRW, Inc. was in violation of the Fair Credit Reporting Act for failing to take adequate steps to protect the privacy of information in its computer data base. The case was settled before trial, precluding a legal interpretation of the metes and bounds of TRW's responsibility.

Citibank N.A. settled a civil action brought by the New York Attorney General's office, based in part on inadequate security for its automated teller machines.

The future of computer crime law is likely to see increasing emphasis on what the computer user can do to protect the data and computer services that make up the heart of the enterprise.

The forward-looking student of data security may well contemplate the fact that the "414 gang" case was used by a number of editorialists to demonstrate the relatively backward state of security awareness on the part of several of the gang's victims.

This attitude could easily translate into increased demands that businesses using computers develop greater security measures on their own or submit to governmental regulation to achieve the same end.

If for no other reason, users should improve their use of existing computer security tools, like computer crime laws, before demands rise for greater governmental involvement in the computer security area. ■

To investigate a crime, call —

As a result of increased activity and increased calls for greater computer security, the number of participants in computer security has grown, offering a number of new choices for a computer security professional trying to decide how to proceed in the investigation or prosecution of a computer crime. Depending on the jurisdiction and the case, any of the following might be helpful.

Local police. Los Angeles, New York, St. Louis and Chicago all have some form of computer fraud unit within their police departments. Many other cities employ individuals who have been trained in computer crime investigations by the Federal Bureau of Investigation, International Association of Chiefs of Police, local attorney generals' offices or private groups. In Silicon Valley, local police departments work together, sharing investigative and educational efforts.

District attorney. A number of areas have had active district attorneys prosecuting computer crime for several years.

In most states with computer crime laws, the district attorney is the prosecutor charged with prosecuting computer crime cases. In many jurisdictions, separate investigative staffs or personnel are attached to a specific unit of the district attorney's office. These investigators may be called on independently of the police investigators.

Which investigator to call is seldom clear. It will usually be determined by cooperation between the prosecutors and investigators who become aware of the case.

Attorney general's office. Though most states vest primary jurisdiction in computer crime prosecutions to district attorneys, attorney generals' offices throughout the country are increasingly becoming involved in computer crime investigations. In most states, the attorney general's office is empowered to investigate any crime and may prosecute the case itself or, more usually, will refer it to the local prosecutor for trial.

FBI. The first law enforcement group to train a large number of its members in computer crime law, the FBI has been active in computer crime investigation for a number of years. The 1984 federal computer crime law stipulates that the FBI and the Secret Service will investigate computer crime cases defined by that law. The law calls for the secretary of the U.S. Department of the Treasury and the U.S. attorney general to draft an agreement spelling out the two organizations' jurisdiction in the area of computer crime.

Secret Service. The Secret Service maintains a traditional role in the investigation of crimes involving counterfeit currency. With the new federal computer crime law, that role will be expanded to include all the computer crimes described in the new law.

U.S. Attorney. The U.S. Attorney's office has prosecuted a number of the major computer fraud cases in history, without relying on computer crime laws. The role of the U.S. Attorney is solely prosecutorial, as the FBI does much of the investigative work.

Professional organizations. Those seeking assistance in the investigation of a computer crime or the application of computer crime laws to a specific situation have a number of nongovernmental sources to call upon for help, including the following:

- The American Society for Industrial Security is the leading professional security organization. Its active National Computer Security Committee consists of a number of experienced computer security professionals.
- The Association for Computing Machinery includes a special interest group on security, audit and control. The group occasionally publishes a newsletter.
- The Computer Security Institute is a private, for-profit organization that organizes a number of computer security-related seminars and publishes a newsletter, a journal and a computer security reference book.
- The Information System Security Association is a nonprofit national group of computer security professionals with local chapters in many cities. They have regular meetings and an annual seminar.
- The National Center for Computer Crime Data is a nonprofit research institute that investigates computer crime, computer security and computer ethics. It publishes a book, the *Computer Crime Law Reporter*; a newsletter, "Conscience in Computing;" and an annual statistical report, "Computer Crime, Computer Security, Computer Ethics."
- MIS Training Institute is a seminar company that offers a number of seminars on computer crime, computer security and all aspects of DP auditing.
- The EDP Auditors Association is a nonprofit organization that publishes a newsletter, sponsors seminars and certifies members as Certified Information Security Analysts if they pass a certification examination.

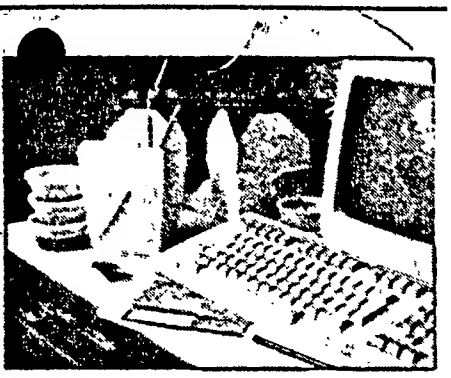
Computer security vendors. Numerous companies are involved in selling computer security products. It is important to point out that these vendors can often offer invaluable assistance in processing a computer crime case, particularly when the case involves an understanding of the operation of the vendors' products.

Victims. Particularly in the case of the telecommunications carriers, victims of computer crime may provide important assistance to other victims or to potential victims. GTE Telenet Communications Corp., for example, has provided significant assistance in a case that resulted in one of the first filings pursuant to the new federal computer crime law. ■

— J. J. BUCK BLOOMBECKER

11/29/85

Portrait of a hacker



GAITHERSBURG, Md. — Tracking a hacker? Look for a boy who eats junk food or Chinese food from 24-hour restaurants.

That is one of the characteristics described by Julie A. Smith, an analyst for the government's National Computer Security Center, at the recent National Computer Security Conference.

Because it is easiest to work on computers undetected during the wee hours of the night, and because many hackers are in school during the day, Smith explained, a hacker's meals tend to be take-out junk food eaten at the computer terminal or food eaten at 24-hour restaurants. "In fact, Chinese food tends to be a favorite among college hackers," Smith said.

This was just one of the characteristics Smith reported in a research paper that provides a psychological profile of the hacker. She said the late hours and self-imposed confinement to computer rooms tend to reinforce the "environmental isolation" of most

See **HACKER** page 65

COMPUTERWORLD

Special Report

Hacker portrait

From page 56

computer hackers.

She said hackers tend to lose interest in schoolwork that is not related to computer science, and thus, their school grades plummet. College-age hackers tend practically to live in the computer buildings on campus.

Smith's research provided additional characteristics of hackers:

- They are almost 100% male.
- Like computer programmers, hackers are extremely bright, investigative and logical thinkers, competitive and prefer structured but creative activities.
- With every successful action at the keyboard, hackers see themselves as asserting authority over the machine and whoever is connected to it, giving them a sense of power and control. Thus, they are more concerned with gaining this sensation of power than they are with the effects of their actions on others.
- Hackers tend to dabble at computer projects with no long-term goal and do not plan ahead.
- Hackers have little respect for those who know nothing about their favorite subject, computers.

"Every aspect of their lives soon becomes linked to computers," Smith said, referring to hackers' social isolation from families and nonhacker friends. "Their speech becomes short and precise in order to avoid any ambiguity in communication, and they often use computer jargon which nonhackers do not understand," she said.

But hackers find refuge in their strong bonds with other hackers, in a hacker culture where individual achievement is highly recognized. "Young hackers love to share information with each other concerning their hacker exploits," Smith said.

In fact, John F. Maxfield, a computer security consultant in Detroit who operates an investigative service called Boardscan, told *Computerworld* that one way to investigate hackers engaged in criminal activity is to catch them bragging about their exploits on electronic bulletin board networks.

The conventional approach to steering hackers away from criminal activity is to lecture them about computer ethics, but this approach has had only mixed success, Smith said. Instead, the social and environmental forces that reinforce hacker behavior must be changed, she asserted.

"It appears as if the best way to combat the narrow-mindedness that young hackers often develop is to change educational patterns so that bright students with an interest in computers are not bored in school," Smith said.

If school is more challenging, teenagers with hacker personality traits may develop interests in subjects like music.

Developing young hackers' interests in noncomputer fields would further develop their intellectual abilities, give them exposure to different environments and enhance their social skills, Smith said. She praised a special Duke University program for talented students that features a balance of challenging academic work and well-planned extracurricular activities.

Furthermore, Smith suggested that "by allowing young hackers to work with computers in an environment where the point of their work is more focused and supervision is available, they would be able to continue to enjoy working with computers at the same time that they are experiencing them as a tool with a purpose beyond the realm of hacking."

— **Mitch Betts**

9/4/87 Chicago, Illinois CG 196B-3287

[redacted] (SECRET SERVICE) b6 b7C

[redacted] 9/8/87

[redacted] was interviewed at his residence, [redacted]

[redacted] had arrived home during the execution of a Federal search warrant. [redacted] and [redacted] had already been interviewed. After [redacted] had been told about the search warrant and had observed the activity taking place in his bedroom and the adjoining computer room, he agreed to be interviewed. By mutual agreement, this interview was conducted in the living room, which is located at the front of the house. [redacted] was advised that no charges had been filed against him, that he was not under arrest and that the interviewing Agents had no intent to arrest him. [redacted] indicated that he knew the reason Agents were in his home.

[redacted] was specifically asked if he had been "hacking". [redacted] replied, "Yeah, what do you want to know?" b6 b7C

[redacted] said that he got into a company computer a long time ago, but it was just a small computer. He advised that computers are hooked up so that they can call each other. He started on UNIX systems some time ago and eventually got into the AT&T system. Information that he learned about one system helped him get into other systems. [redacted] described this as a "chain reaction".

[redacted] has called a lot of different numbers, possibly between 500 and 600, all around the country. For the most part, he has not called numbers which have been publicized on computer bulletin boards. He has not used publicized numbers because that would run the "risk of something like this".

Originally, his only interest in getting into other computers was for the sake of exploring. Later, he wanted to learn the languages on these other machines.

[redacted] was asked if he used any aliases when he was hacking. He indicated that he did. He was therefore asked what names he used. [redacted] replied that the only name he has been using recently is [redacted] which is a name he found [redacted] Previously he has used [redacted] or simply [redacted] was specifically asked if he had ever heard of a hacker who used the name [redacted] indicated that he had not. b6 b7C

196B-1-2

Searched Serialized Indexed Filed [redacted]

QT 196B-1

[redacted]

[redacted] was asked if he had called the BELL LABORATORY at Indian Hill. [redacted] said that he had. He was then asked if he had managed to get into a computer known as [redacted] [redacted] replied that he knows [redacted] but that he never got into it. He was therefore asked if he had ever masqueraded as [redacted] Smiling, [redacted] replied "Um, hmm". [redacted] stated that with AT&T UNIX machines he did masquerade as [redacted] He added that the local system at Indian Hill is [redacted] but the model number is [redacted] [redacted] volunteered that he had gained access to a lot of other AT&T computers. When asked how many, he replied that they were "innumerable". [redacted] said that on his computer he did have a list of some of the other AT&T computers he had entered. [redacted] stated that he has used a data network which links AT&T computers. With it, he has hopped around all over.

b6
b7C
b7E

He was asked if he had ever gained access to AT&T computers in New Jersey. He replied that he had, a couple of times. He was also asked if he had gained entry to AT&T computers in North Carolina. He replied that he did not specifically recall getting on a computer there. He observed that he has a friend, [redacted] Last Name Unknown (LNU), who lives in North Carolina. [redacted] has never met [redacted] in person. It is possible that [redacted] was on a computer in another state and did not realize it. He observed, however, that he generally knew at least the state in which a computer was located.

[redacted] was asked if he had ever gained access to the VAX system at MIT. He replied that he had on a couple of occasions. [redacted] observed that it was easy to get on that computer. When he dialed the number he discovered that the previous user of a non-privileged account had not disconnected properly. As a result, he was in the computer as soon as he dialed the number. [redacted] did get out software from that computer.

b6
b7C

[redacted] stated that when he got into these computers, he wanted to look at the way AT&T programmed the computers. He wanted to see how programming was done professionally. As far as he knows, [redacted] did not obtain any national defense secrets. The information he removed is scattered through his computer. He keeps information on his hard drive, not on floppy disks.

As far as he knows, [redacted] did not get on a computer at an Air Force base and did not obtain information about AUTOVON, the military communication network. He stated that he almost got on ARPANET, which he described as a defense data network. He believes that system may be connected to the VAX computer at MIT.

b6
b7C

[redacted] was asked if he had ever taken an artificial intelligence program from an AT&T computer. He replied that as far as he knows, he did not. He did get from one AT&T computer a program named [redacted] which had to do with visual screen activities. He said that he got other programs from AT&T including EMACS, KORN SHELL, and E SHELL. [redacted] observed that E SHELL was not very important.

b7E

[redacted] was then asked what he did with all of this material. He replied that he kept it to himself pretty much. He said that he never sold any of these programs. He used these programs only for his own education. [redacted] also stated that he did not let anybody copy the programs which he had obtained. [redacted] noted that three of his friends do have telephonic access to his computer because he has given them the proper password. As far as he knows, these friends have not taken any of the software he obtained. With the materials he obtained, he has been learning some things like programming in "C". [redacted] stated that he has not completely mastered programming in "C". b6 b7C

[redacted] was asked if he had ever been able to get into the AT&T program called COSMOS. He replied that he had not.

[redacted] was next asked if he had ever used unauthorized access codes to obtain long distance telephone services for free. He replied that several times he has used codes from numerous long distance services to avoid long distance charges. He has for example used an access number for ALLNET. He does not have an ALLNET account; he got the access number from a computer bulletin board. [redacted] has also used an access number to get service from SPRINT. [redacted] observed that it is better to use access numbers for long distance service that have been listed on public computer bulletin boards. Such numbers are used by many people, so it is virtually impossible to be prosecuted. The real risk of prosecution would arise if you were to hack out such an access number by yourself. Since you would be the only person using that number, it would be easier to identify you and to prosecute you. [redacted] knows that it is illegal to use such access numbers.

[redacted] was also asked about his knowledge of the law regarding the software he obtained from AT&T computers. [redacted] replied that he has noticed the copyright statements which appear in the AT&T computers. He knows that it is illegal to copy those programs but he added that he has not distributed those programs. He did not post the information he got on computer bulletin boards. He observed that the first time he got in trouble, the problem resulted from the fact that he did post information. b6 b7C

The first time he got in trouble was when he broke into computers belonging to the KELLER BUSINESS SCHOOL and to a brokerage company whose name he no longer recalls. Both used an RSTS system. He did not do anything to the computers while he was in them and he did not do anything with the information he obtained. He did, however, post information on a bulletin board. Someone else called up those computers and shut them off. As a result, the CHICAGO POLICE DEPARTMENT came to his home. This happened when he was 15 or 16 years old.

[redacted] did not have to go to court as a result of that incident. He was told that the offense was less than a misdemeanor. At the time, he offered his services in explaining b6 b7C

to representatives of KELLER how he had gained access to the computer. His offer was not accepted because it became obvious to them how he had gained access. [redacted] explained that he had used a "default password". He stated that computer manufacturers place passwords in the system before the computer is delivered to a user. Unless a user like KELLER removes those passwords, anyone can gain access to the computer by using one of those passwords. b6 b7C

[redacted] identified [redacted] as another computer hacker who was involved with him in breaking into the KELLER computer. [redacted] does not recall [redacted] address but knows that [redacted] lives near the [redacted] in Chicago. [redacted] did not participate with [redacted] in recent break-ins on AT&T computers. As far as [redacted] knows, [redacted] is not familiar with UNIX.

[redacted] stated that he did not think anything would come of the "AT&T stuff". [redacted] believed this because he tried not to leave any record of his entry into the computer. He said he tried to cover his tracks as best as he could. He believed that the best chance he would have of being caught would come from an examination of long distance telephone or local telephone records. He noted that he was implicated in the KELLER incident on the basis of local telephone records. b6 b7C

[redacted] was next asked if he had ever engaged in the use of "Trojan Horses". He replied that he had not made any trojan horses and had not left any behind in the computers he had entered.

[redacted] was next asked why he had made calls to Pipe Creek, Texas. He replied that he had hacked into a guy's system there. The guy was friendly about it and let [redacted] continue to enter the system. This guy had access to a free message system called USENET. [redacted] observed that a lot of it was run by AT&T. b6 b7C

[redacted] was next asked if he was a member of the Phreak Class 2600 computer bulletin board. [redacted] replied that yes, that was one of the bulletin boards he used. He added, however, that he has not called that bulletin board for about 1 month. At this point, [redacted] was again confronted with his knowledge of [redacted] When confronted with the possibility that he, in fact, was [redacted] admitted that he was. [redacted] assured the Agents that this was the only subject matter he had lied about during the course of the interview.

[redacted] was asked if he realized that he could have caused significant problems to the communications network while he was exploring AT&T computers. [redacted] replied that he did realize he could have caused some problems, but as far as he knows, he did not. [redacted] again stated that all he really wanted to do was to learn. He has been told that AUTOVON is a separate system from the one which you can dial up. He has not knowingly ever been on the AUTOVON system. As far as he knows, he has not obtained b6 b7C

information about AUTOVON or about NATO. [redacted] claimed that one would need inside information in order to get on COSMOS. Accordingly, he has not really tried to get in on the COSMOS system. Another reason he did not try to get into COSMOS was the fact that it was supposedly used only to keep track of maintenance records for the telephone company.

The only information [redacted] distributed was that which was already public. [redacted] stated that he has a UNIX 3B1 computer which was bought at a ham fest. b6 b7C

At this point in the interview, [redacted] was asked to examine copies of two messages which had been left by [redacted] on bulletin boards. After reading the message dated May 10, [redacted] stated "I did post that". [redacted] placed his initials before and after that message to identify the portion he recognized. The second message was contained on two pages. [redacted] recognized it as a message he had posted on the RIPCO bulletin board. [redacted] also initialed the beginning and end of this message to identify it.

[redacted] observed that he would not post anything valuable he had learned by hacking on one of the computer bulletin boards. It would not make any sense to post valuable information on a bulletin board because it would die too fast. It would be used just like the access numbers for long distance service. Generally, if [redacted] was going to post any information he would do it on the RIPCO bulletin board. [redacted] asserted that he never wanted to cause any damage to a computer or to use a system against people. In his mind, he was "just touring systems". At the conclusion of this interview, [redacted] went to his room in order to offer assistance to Agents and to representatives of AT&T who were still examining his computer. b6 b7C

The following description was obtained by observation and interview:

Name	
Sex	
Race	
Date of birth	
Place of birth	
Height	
Weight	
Eyes	
Hair	
Hair style	
Scars, marks or tattoos	

b6 b7C

[redacted] did not remember his Social Security Account Number. He has an Illinois driver's license but he had to surrender that recently when he had an accident. b6 b7C

2-224 (13-17-87)

BEHAVIORAL SCIENCE SERVICES ACCOMPLISHMENT REPORT

*To: MR. [redacted] *Date: 2/20/88 File#: QT 196B-1

☐ Foreign ☐ Domestic ☒ Bureau ☐ Other

*From: [redacted] Date of Activity: 2/20/88 Total Hours: 1/2

b6
b7C

*Subject: [redacted]

AKA [redacted]

FRAUD BY WIRE

(00: CHICAGO)

Case Assigned To: [redacted] Unit Member (s): _____

* ☐ BSIRU ☐ BSISU ☒ BSCES ☐ POLICE FELLOWS

*Program: ☐ RESEARCH ☐ TRAINING ☐ VICAP ☒ PROFILE/CONSULTATION ☐ OTHER

* ☐ TELEPHONIC ☐ WRITTEN ☐ ON-SITE ☒ QUANTICO

Instruction Provided
- ☐ Field School
- ☐ Faculty Development
- ☐ Student Counselling
- ☐ Conference/Seminar
- ☐ Consultation
- ☐ New Agents
- ☐ National Academy
- ☐ DEA
- ☐ In-Service
- ☐ Preparation
- ☐ Role Playing
- ☐ Symposium
- ☐ Speaking Engagement
- ☐ Other _____
- ☐ Topic _____
- _____
- ☐ #Departments _____

Investigative
- ☒ Consultation
- ☐ Profile
- ☐ Personality Assessment
- ☐ Investigative Techniques
- ☐ Interview Strategy
- ☐ Trial Strategy
- ☐ Testimony
- ☐ Crime Analysis
- ☐ Equivocal Death
- ☐ #Victims ____
- ☐ #Subjects ____
- ☐ #Suspects ____

VICAP
- ☐ Crime Analysis
- ☐ Consultation
- ☐ Linkage

Research
- ☐ Unpublished Paper/Handout/etc.
- ☐ Publication (Article/Book/etc.)
- ☐ Original Research/Academic Citation
- ☐ Interview
- ☐ Consultation

Administrative
- ☐ Meeting
- ☐ Media/Publicity
- ☐ Liaison
- ☐ Field Support
- ☐ Travel
  Time _____
- ☐ Consultation
- ☐ Psychological Service
- ☐ Organization Membership
- ☐ Awards/Honors/Letters
- ☐ Organizational Coop.
- ☐ Other _____

Computer Support
- ☐ Programming
- ☐ Data Analysis
- ☐ System Development
- ☐ Consultation
- ☐ Technical Assistance

Instruction Received
- ☐ In-Service
- ☐ Non-FBI

Project
- ☐ New
- ☐ Pending
- ☐ Closed

Other: _____

b6
b7C

[redacted]

Class Description
#Of Students: ____ Student Type: _____ Instruction Hours: ____

196B-1-3

Distribution
1- _____
1- _____
1- _____

Searched
Serialized
Indexed
Filed

FBI/DOJ

SUMMARY: NO FURTHER COMMUNICATIONS HAVE BEEN RECEIVED FROM CHICAGO DIVISION REQUESTING INVESTIGATIVE ASSISTANCE. REVIEW OF FILE ALSO INDICATES NO ADDITIONAL ASSISTANCE CAN BE PROVIDED AT THIS TIME.

☐ See Attached

COMMENTS/RECOMMENDATIONS: CLOSE CASE.

Field Office Appraisal Criteria-

Executive Management:

Supervision, Evaluation, Development of Subordinates:

Liaison and Media Relations:

*Mandatory Field

2-224 (11-17-87)

BEHAVIORAL SCIENCE SERVICES ACCOMPLISHMENT REPORT

*To: MR. [redacted] *Date: 3/3/89 File#: QT 196B-1

☐ Foreign ☐ Domestic ☒ Bureau ☐ Other

*From: [redacted] Date of Activity: 3/2/89 Total Hours: 2

b6
b7C

*Subject: [redacted]
AKA [redacted]
FRAUD BY WIRE;
OO: CHICAGO

Case Assigned To: [redacted] Unit Member (s): _____

* ☐ BSIRU ☐ BSISU ☒ BSCES ☐ POLICE FELLOWS

*Program: ☐ RESEARCH ☐ TRAINING ☐ VICAP ☒ PROFILE/CONSULTATION ☐ OTHER

* ☐ TELEPHONIC ☐ WRITTEN ☐ ON-SITE ☐ QUANTICO

Instruction Provided
- ☐ Field School
- ☐ Faculty Development
- ☐ Student Counselling
- ☐ Conference/Seminar
- ☐ Consultation
- ☐ New Agents
- ☐ National Academy
- ☐ DEA
- ☐ In-Service
- ☐ Preparation
- ☐ Role Playing
- ☐ Symposium
- ☐ Speaking Engagement
- ☐ Other _____
- ☐ Topic _____
- ☐ #Departments _____

Instruction Received
- ☐ In-Service
- ☐ Non-FBI

Other: _____

Investigative
- ☒ Consultation
- ☐ Profile
- ☐ Personality Assessment
- ☐ Investigative Techniques
- ☐ Interview Strategy
- ☐ Trial Strategy
- ☐ Testimony
- ☐ Crime Analysis
- ☐ Equivocal Death
- ☐ #Victims ____
- ☐ #Subjects ____
- ☒ #Suspects 1

1 CONVICTION

VICAP
- ☐ Crime Analysis
- ☐ Consultation
- ☐ Linkage

Project
- ☐ New
- ☐ Pending
- ☐ Closed

Research
- ☐ Unpublished Paper/Handout/etc.
- ☐ Publication (Article/Book/etc.)
- ☐ Original Research/Academic Citation
- ☐ Interview
- ☐ Consultation

Administrative
- ☐ Meeting
- ☐ Media/Publicity
- ☐ Liaison
- ☐ Field Support
- ☐ Travel
- Time _____
- ☐ Consultation
- ☐ Psychological Service
- ☐ Organization Membership
- ☐ Awards/Honors/Letters
- ☐ Organizational Coop.
- ☐ Other _____

Computer Support
- ☐ Programming
- ☐ Data Analysis
- ☐ System Development
- ☐ Consultation
- ☐ Technical Assistance

Class Description
#Of Students: ____ Student Type: ☆ State Instruction Hours: ____

Claim conviction re fraud by wire.

196B-1-4

Distribution
1- MR [redacted]
1- MR
1- QT 196B-1
1- QT 252C-C2187
✓ [redacted]

Searched
Serialized
Indexed
Filed

[redacted]

b6
b7C

FBI/DOJ

SUMMARY: ATTACHED IS A SUMMARY OF CAPTIONED CASE. THE SUBJECT WAS CONVICTED 1/23/89 IN CHICAGO AND IS THE FIRST UNDER THE "COMPUTER FRAUD AND ABUSE ACT of 1986." AUSA [redacted] WAS CONTACTED, AND HE WILL TRY TO OBTAIN A COURT ORDER TO RELEASE DOCUMENTS TO THE NCAVC IN ANTICIPATION OF INTERVIEWING THIS SUBJECT IN THE "COMPUTER SECURITY AND CRIME RESEARCH PROJECT." IDENTIFICATION INFORMATION IS CONTAINED BELOW:

b6
b7C

- FBI IDENTIFICATION RECORD -

WHEN EXPLANATION OF A CHARGE OR DISPOSITION IS NEEDED, COMMUNICATE DIRECTLY WITH THE AGENCY THAT FURNISHED THE DATA TO THE FBI.

NAME	FBI NO.	DATE REQUESTED
[redacted]	[redacted]	03/03/89

SEX	RACE	BIRTH DATE	HEIGHT	WEIGHT	EYES	HAIR	BIRTH PLACE
[redacted]							

b6
b7C

FINGERPRINT CLASS

[redacted]

☒ See Attached

COMMENTS/RECOMMENDATIONS: NONE. FOR INFORMATION ONLY.

Field Office Appraisal Criteria-

Executive Management:

Supervision, Evaluation, Development of Subordinates:

Liaison and Media Relations:

*Mandatory Field

3/1/89

Mr. [redacted]

RE: [redacted] b6 b7C
AKA [redacted]
FBW;
OO: CHICAGO

On 1/23/89, Judge Paul E. Plunkett, U.S. District Court for the Northern District of Illinois, found [redacted] on five of the six counts of violation of Title 18, U.S. Code, Section 1030, Fraud and Related Activity in Connection with Computers. On 2/14/89, Judge Plunkett sentenced [redacted] to nine months in jail, followed by a period of probation to end on 8/6/91, [redacted] In addition to this sentence and probation, [redacted] was also ordered, within his ability, to pay $10,000 in restitution. b6 b7C

The underlying criminal information charged that between 7/87 and 9/87, 18-year-old [redacted] unlawfully entered computers owned and operated by AT&T and the U.S. Government, and illegally copied proprietary AT&T software valued in excess of $1.2 million, causing $174,000 worth of damage to AT&T computers. During the course of the one-week bench trial in 1/89, the Government's evidence also established that in 5/87 and 6/87, the defendant published passwords to AT&T computers on computer bulletin boards in Chicago and Texas. b6 b7C

On 9/4/87, a search warrant was executed on [redacted] residence at which time his computer was recovered along with 52 of the AT&T copyrighted software programs which had been stolen from Bell Laboratory and North Atlantic Treaty Organization computers. b6 b7C

The case was prosecuted by Assistant U.S. Attorney William J. Cook, and was the first trial ever brought under the Computer Fraud and Abuse Act of 1986.

[redacted] b6 b7C

1 - Mr. [redacted]
1 - Mr. [redacted]
(Attn: Dr. [redacted])
1 - Mr. [redacted]
1 - Mr. [redacted]
1 - Mr. [redacted]
1 - Mr. [redacted]
1 - Mr. [redacted]
1 - Special Assistants, CID

[redacted] (10)

2-222 (7-15-85)

CASE STATUS FORM

CASE TITLE

[redacted]

aka [redacted]

FRAUD BY WIRE;
(OO: CHICAGO)

Quantico File No. QT 196B-1

Office of Origin CHICAGO

OO-File No. 196B-3287

Profile Coordinator

Requesting Agency/Investigator SA [redacted]

Telephone No. FTS: 380-6015

Acknowledgement Letter (Date Sent)

b6
b7C

CASE MANAGEMENT

ASSIGNMENT: CASE SUPERVISOR [redacted]

LEADS

DATE CASE RECEIVED: 10/2/87

VI-CAP FORM SUBMITTED ☐ YES ☒ NO VI-CAP CASE NO.

DATES OF FILE REVIEWS / / /

SYNOPSIS OF CRIME: JOINT FBI/USSS INVESTIGATION INTO POSSIBLE VIOLATIONS OF 18USC 1030 (FRAUD AND RELATED ACTIVITIES IN CONNECTION WITH COMPUTERS)

SPECIFIC REQUESTS FOR CASE ASSISTANCE

PROFILE ☐ YES ☒ NO DATE PROVIDED

INVESTIGATIVE TECHNIQUES ☒ YES ☐ NO

	DATE
POSSIBLE FBI JURISDICTION, ARTICLES ON COMPUTER FRAUD	10/2/87

INTERVIEW/ INTERROGATION TECHNIQUES ☐ YES ☒ NO

PROSECUTIVE STRATEGY ☒ YES ☐ NO RESTITUTION, BILL OF INFORMATION

TESTIMONY ☐ YES ☒ NO NAME OF PROSECUTOR

ASSESSMENT OF SUSPECT ☐ YES ☒ NO DATE PROVIDED

CASE CONSULTATIONS
(ON-SITE, FBIHQ, FBI ACADEMY, TELEPHONIC)

DATE	NOTES
10/2/87	INITIAL CALL TO BSISU BY SA [redacted] ARTICLES & INFO SENT VIA MAIL CHICAGO WILL CALL IF ADDITIONAL INFO IS NEEDED AND IS CHECKING WITH LOCAL PROSECUTOR TO DECIDE JURISDICTION. SUBJECT IS [redacted]

b6
b7C

FBI/DOJ